## AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method for combating spam comprising:

classifying a message at least partially by evaluating at least one message parameter, using at least one stored parameter template, thereby providing a spam classification, said using comprising using said at least one stored parameter template at at least one gateway and said providing comprising providing said spam classification at at least one server, said at least one server being operative to periodically provide updated parameter templates to said at least one gateway, said at least one server receiving evaluation outputs from said at least one gateway and providing said spam classification to said at least one gateway; and

handling said message based on said spam classification.

2. (Previously Presented) A method for combating spam according to claim 1 and wherein said at least one stored parameter template comprises a parameter template which changes over time.

3-4. (Cancelled)

5. (Currently Amended) A method for combating spam according to ~~claim 1~~ claim 1 and wherein said classifying also comprises:

encrypting at least part of said evaluation outputs by employing a non-reversible encryption so as to generate encrypted information; and

transmitting at least said encrypted information to said at least one server.

6. (Original) A method for combating spam according to claim 5 and wherein said transmitting comprises transmitting information of a length limited to a predefined threshold.

7. (Previously Presented) A method for combating spam according to claim 1 and wherein said handling comprises at least one of:

forwarding said message to an addressee of said message;

storing said message in a predefined storage area;

deleting said message;

rejecting said message;

sending said message to an originator of said message; and

delaying said message for a period of time and thereafter re-classifying said message.

8. (Previously Presented) A method for combating spam according to claim 1 and wherein said message comprises at least one of:

an e-mail;

a network packet;

a digital telecom message; and

an instant messaging message.

9. (Previously Presented) A method for combating spam according to claim 1 and wherein said classifying also comprises at least one of:

requesting feedback from an addressee of said message;

evaluating compliance of said message with a predefined policy;

evaluating registration status of at least one registered address in said message;

analyzing a match among network references in said message;

analyzing a match between at least one translatable address in said message and at least one other network reference in said message;

at least partially actuating an unsubscribe feature in said message;

analyzing an unsubscribe feature in said message;

employing a variable criteria;

sending information to a server and receiving classification data based on said information;

employing classification data received from a server; and

employing stored classification data.

10. (Currently Amended) A method for combating spam comprising:

classifying messages at least partially by evaluating at least one message parameter of multiple messages, by employing at least one stored parameter template which changes over time, thereby providing spam classifications, said employing at least one stored parameter template comprising using said at least one stored parameter template at at least one gateway; and said providing spam classifications comprising providing said spam classifications at at least one server, said at least one server being operative to periodically provide updated parameter templates to said at least one gateway, said at least one server receiving evaluation outputs from said at least one gateway and providing said spam classification to said at least one gateway; and

handling said messages based on said spam classifications.

11. (Original) A method for combating spam according to claim 10 and wherein said classifying is at least partially responsive to similarities between plural messages among said multiple messages, which similarities are reflected in said at least one message parameter.

12. (Previously Presented) A method for combating spam according to claim 10 and wherein said classifying is at least partially responsive to similarities between plural messages among said multiple messages, which similarities are reflected in outputs of applying said at least one stored parameter template to said at least one message parameter.

13. (Previously Presented) A method for combating spam according to claim 10 and wherein said classifying is at least partially responsive to similarities in multiple outputs of applying a single stored parameter template to said at least one message parameter in multiple messages.

14. (Previously Presented) A method for combating spam according to claim 10 and wherein said classifying is at least partially responsive to the extent of similarities between plural messages

among said multiple messages which similarities are reflected in said at least one message parameter.

15. (Previously Presented) A method for combating spam according to claim 10 and wherein said classifying is at least partially responsive to the extent of similarities between plural messages among said multiple messages which similarities are reflected in outputs of applying said at least one stored parameter template to said at least one message parameter.

16. (Previously Presented) A method for combating spam according to claim 10 and wherein said classifying is at least partially responsive to the extent of similarities in multiple outputs of applying a single stored parameter template to said at least one message parameter in multiple messages.

17. (Previously Presented) A method for combating spam according to claim 14 and wherein said extent of similarities comprises a count of messages among said multiple messages which are similar.

18. (Previously Presented) A method for combating spam according to claim 10 and wherein said classifying is at least partially responsive to similarities in outputs of applying stored parameter templates to said at least one message parameter in multiple messages, wherein a plurality of different stored parameter templates are individually applied to said at least one message parameter in said multiple messages, yielding a corresponding plurality of outputs indicating a corresponding plurality of similarities among said multiple messages.

19. (Original) A method according to claim 18 and wherein said classifying also comprises aggregating individual similarities among said plurality of similarities.

20. (Original) A method according to claim 19 and wherein said aggregating individual similarities among said plurality of similarities comprises applying weights to said individual similarities.

21-186. (Cancelled)

187. (New) A method for combating spam according to claim 1 and wherein said evaluating includes calculating a value based on said at least one message parameter.

188. (New) A method for combating spam according to claim 1 and also comprising:

categorizing incoming messages received at said at least one gateway into at least first, second and third categories;

providing spam classifications for incoming messages in at least said first and second categories;

not immediately providing a spam classification for incoming messages in said third category;

delaying said incoming messages in said third category for a period of time and thereafter re-classifying said messages based on classifications of incoming messages received during said period.

189. (New) A method for combating spam according to claim 1 and also comprising classifying said message at least partially by relating to an unsubscribe feature in the message, thereby providing said spam classification for said message.

190. (New) A method for combating spam according to claim 1 and also comprising classifying said message at least partially by relating to a registration status of at least one registered address in said message, thereby providing said spam classification for said message.

191. (New) A method for combating spam comprising:

classifying a message at least partially by evaluating at least one message parameter, using at least one stored parameter template, thereby providing a spam classification, said using at least one stored parameter template comprising using said at least one stored parameter template at at least one gateway and said providing a spam classification comprising providing said spam classification at at least one server, said at least one server receiving evaluation outputs from said at least one gateway and providing said spam classification to said at least one gateway, said evaluating including calculating a value based on said at least one message parameter; and

handling said message based on said spam classification.

192. (New) A method for combating spam comprising:

categorizing incoming messages received at at least one gateway into at least first, second and third categories;

providing spam classifications for incoming messages in at least said first and second categories;

not immediately providing a spam classification for incoming messages in said third category;

delaying said incoming messages in said third category for a period of time and thereafter re-classifying said messages based on classifications of incoming messages received during said period; and.

handling said incoming messages based on said spam classifications.

193. (New) A method for combating spam comprising:

classifying a message at least partially by relating to an unsubscribe feature in the message, thereby providing a spam classification for said message; and

handling said message based on said spam classification.

194. (New) A method for combating spam comprising:

classifying a message at least partially by relating to a registration status of at least one registered address in said message, thereby providing a spam classification for said message; and

handling said message based on said spam classification.